EXHIBIT
(U.S. Provisional Patent Application Serial No. 60/517,868 of Golan et al.)

Please type a plus sign (+) inside this box →

PTO/SB/16 (8-00)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Lior	GOLAN	Tel Aviv, Israel
Naftali	BENNETT	New York, NY
Nira	RIVNER	Herzelia, Israel
Michal	TSUR	Baltimore, MD
Amir	ORAD	Shoham, Israel

☐ *Additional inventors are being named on the ^ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (280 characters max)

SYSTEM AND METHOD OF ADDRESSING EMAIL AND ELECTRONIC COMMUNICATION IDENTITY FRAUD

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☒ Customer Number 27130 → *Place Customer Number Bar Code Label here*

OR *Type Customer Number here*

☒ Firm or Individual Name	Eitan, Pearl, Latzer & Cohen Zedek, LLP.				
Address	10 Rockefeller Plaza				
Address	Suite 1001				
City	New York	State	New York	ZIP	10020
Country	USA	Telephone	212-632-3480	Fax	212-632-3489

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 11 ☐ CD(s), Number

☐ Drawing(s) *Number of Sheets*

☐ Application Data Sheet. See 37 CFR 1.76 ☒ Other (specify) postcard

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

☒ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 05-0649

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($): 80

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME Cal b Pollack

TELEPHONE 212-632-3480

Date 07 / Nov / 2003

REGISTRATION NO. *(if appropriate)* 37,912

Docket Number: P-6325-USP

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the

UNITED STATES PROVISIONAL PATENT APPLICATION FOR:
SYSTEM AND METHOD OF ADDRESSING EMAIL AND ELECTRONIC COMMUNICATION IDENTITY FRAUD

Embodiments of the present invention relate to a method and system for filtering electronic mail ("e-mail") sent to one or more users via a communications network. The system and method may alert individuals and organizations ("Service Providers") against identity fraud and brand impersonation in the form of unsolicited e-mail messages that appear to be originating from those individuals or organizations (this new phenomena is referred to as "Phishing"). The system and method may enable the removal of such email messages from recipients' mailboxes, to alert recipients against any such fraud, to alert law enforcement officials against such fraud, and also to reduce negative consequences associated with the submitting of valuable and confidential information by individuals to fraudulent impostors. .

BACKGROUND:

The rapid increase in the number of users of electronic mail and the low cost of distributing electronic messages via the Internet and other electronic communications networks has made marketing and communications with existing customers via e-mail an attractive advertising medium. Consequently, in addition to communications that are warranted by consumers, e-mail is now frequently used as the medium for unsolicited widespread communication and marketing broadcasts of messages to e-mail addresses, commonly known as "Spam".

"Phishing" or Email identity fraud and brand impersonation are the newest forms of harmful Spam attacks that threaten the integrity of companies doing business online. Fraudulent (Phishing) email messages may be considered to be, for example, messages that appear to be sent from a legitimate company's website or domain address, but in fact

are not. In reality, Spammers are hijacking the company's brand to attract the attention of customers, often to gain personal information.

Lately several banks and other companies have been attacked by Phishing. For the sake of example, and without limiting the generality of the phenomena, if a bank is attacked by phishing, individuals may receive an email which is allegedly sent by the bank, and are persuaded into supplying private (valuable) identifying personal data online under several pretences – for example (without limitation) – so that the bank can register them to a new service, or to protect against unauthorized charges.

The damage to the bank, or any other company whose identity if faked is significant – Phishing can injure valuable corporate brand equity, ruin customer trust, increase operational costs through growing customer complaints, and pose potential legal risks from not adequately protecting the corporate trademarks. The bank or other attached company usually has to publish a general warning to its customers, and sometimes even cancel or block people's accounts.

An additional problem spamming causes is that many Internet Service Providers (ISPs) have implemented an anti-spam service. This service blocks e-mails that are suspected of being spam from reaching the end-user. At times, these spam blockers have "false positives" – legitimate e-mails that are flagged as spam. Service Providers may find that a legitimate email message sent to their customers was blocked because it was sent to a large distribution list, or because it included words such as "free", or other anti-spam-triggering features.

Phishing may involve, for example:

1. The originators of "Phishing" emails attempt to make the email distributed seem to be coming from a legitimate source. In order to achieve that goal, the Phishing email is usually disguised as a legitimate email, and includes elements and characteristics of a legitimate organization, such as (without limitation) logo, domain names, brands and colors.

2. In order for the phishing to be advantageous for its originators, the originators of "phishing" need to somehow divert information that the trusting consumers submit in response to the seemingly legitimate email. Such information might be diverted via for example a link to a separate web-page that requires the individual to input valuable private information, or via telephone, if the email directs the recipient to call a certain telephone number (following which the recipients valuable information might be collected over the phone). Such illegitimate links or contact telephone numbers shall be referred to as "illegitimate contact pointers".

The implications of the above characteristics of phishing are that any Phishing emails typically include a mixture of both legitimate and illegitimate contact pointers (such as links to other web pages or telephone numbers). Legitimate contact pointers would point to web pages or telephone numbers that belong to legitimate email senders. Illegitimate contact pointers would point to web pages or telephone numbers that belong to the fraudsters.

The goal of a useful anti-phishing method/ service would include, for example, any or all of the following:

1. Detection of potential phishing scams
2. Configuration options to allow the bank to define phishing detection parameters
3. Alert of the bank of the detected scam, including a sample of the phishing email
4. Option for the bank to request for:
    a. Blocking of the phishing email before it reaches the recipients' mailboxes
    b. Alert to cardholders' emails
    c. Alert to law enforcing authorities
    d. Approval of the mail as an official email by the bank (non-phishing)
5. Phishing reports
6. Training and support for the internal user of the APS (Anti Phishing Service; while APS is used herein other nomenclatures may be used, and embodiments of the present invention may include systems and methods working with situations other than "Phishing") at the bank

7. Maintenance of "white lists" of legitimate email campaigns to make sure they are not flagged as spam.
8. Tools for minimizing the impact of the Phishing scam, as well as tools that would facilitate detecting the Phishing originators.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described. For purposes of explanation, specific configurations and details are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details presented herein. Furthermore, well-known features may be omitted or simplified in order not to obscure the present invention. Various examples are given throughout this description. These are merely descriptions of specific embodiments of the invention, but the scope of the invention is not limited to the examples given.

Embodiments of the invention may be used so that organizations will be alerted against Phishing or other fraudulent email or other electronic communication, and so that Phishing emails or other communications will be blocked or otherwise dealt with, for example without reaching recipients' mailboxes.

According to one embodiment of the present invention a list of legitimate contact pointers which might include, but is not limited to, domain names, links, telephone numbers, fax numbers and logos is maintained. Such list may be maintained and updated frequently, both by the organizations actively, as well as in response to the utilization of the system described herein (e.g., after the system mistakenly alerts against a Phishing email, the contact pointers that appeared to the system to be illegitimate shall be added to the list of legitimate contact pointers).

There may be established a list of rules intended to identify and filter emails or other electronic communications that may include a mixture of legitimate contact pointers and illegitimate ones (including without limitation domain names, links, telephone numbers, fax numbers and logos). The system utilizing such rules may be able to identify phishing emails or other communications, and to consequently flag such emails, and alert against them once such emails are identified by the rules. Further rules, such as a second set of secondary rules, as well as potentially human review, may applied to all emails that were flagged as Phishing emails, in order to insure that no emails were falsely characterized as Phishing emails. If based on such secondary rules and/ or reviews

of emails that were flagged by the system as Phishing emails, the flagged emails shall be found legitimate – the system will update its list of legitimate contact pointers to include the new ones that were flagged as illegitimate.

For example, without limiting the foregoing the system could apply the following rule in order to identify a Phishing email:
If a message includes at least one legitimate contact pointer, and at least one illegitimate contact pointer, the message will be flagged as an email that is potentially part of a Phishing scam. The rules could require fewer or more elements of legitimate or illegitimate contact pointers, could be focus on various types of contact pointers (such as checking only domain names).

In addition a list of legitimate emails, or sender email addresses, or origin domain names may be compiled so as to form a "white list", or other suitable data structure, which is typically always approved by the system.

In order to set up such a service it may be necessary to collect with respect to each Service Provider or other organization that seeks protection against Phishing any or all of the following, or other suitable information:

1. A list of legitimate domains, including those of approved vendors.
2. A list of trademarks and service names
3. A list of customer service and marketing related phone numbers
4. Contact info for the relevant people and departments at the Service Provider to handle phishing incidents
5. Possibly also specific emails used as part of the Service Provider's campaigns to make sure they enter a "white list" that will not be flagged as spam

The collection may be done for example in a manual form, or via a web interface.

The detection of phishing scams can be done using existing anti email-spam methods which can issue alerts whenever they detect an email, which contains at least X (e.g., a suitable number, where one may be a suitable number) legitimate contact pointers such as domains/trademarks/service names/phone numbers by the Service Provider, along

with illegitimate pointers. (one such anti email-spam method is called **"honey pots"** or **"decoys"**. An anti email-spam company that works with this method may set up numerous email accounts that do not belong to real people or entities, and lists them in public email guides. If an email gets to these addresses it can be either the result of a spam or an honest mistake. If the email reaches several addresses the chances of an honest mistake are slim. Other methods may include for example content filtering or sniffing.)

Once a potential phishing scam or other unwanted data communication is identified the system may perform some pre-processing to make sure it is indeed a suspicious email or communication. At this point the Server can also contact ISPs or other organizations and for example anti-spam companies asking for the quarantine of the message.

At this point the system can also route an alert to the appropriate Service Provider. The alert may also include a copy of the original email as detected. The alert can be delivered by for example email or via a web interface, or other suitable method. The alert also may include an estimate of the size of the phishing scam.

The Service Provider or other organization may review the incoming alerts. It can then either determine whether it is a legitimate message and request to remove the alert (and the possible quarantine), or determine it is indeed a phishing attempt or other unwanted communication. A Service Provider may be able to achieve any one or more of the following, although other results are anticipated according to embodiments of the invention:

1. block the message - the APS server (or another suitable server) contacts ISPs and anti-spam companies and requests for the blocking of the message
2. alert the law enforcement authorities so that they can work to block the web site or the origin account sending the emails
3. send an alert to the Service Provider customers via email
4. **Clogging:** For example, the Phishing website to which tries to collect data from the Service Provider's customers, is filled with fake records of people, thus diluting the quality of data that the fraudsters obtain.

5. **Mark & Block**: For example, the Phishing website to which tries to collect data from the Service Provider's customers, is filled with fake records of people. When the Service Provider detects that those "fake people" attempt to access the Service Provider's *real* website/ Service, it will be possible to identify the source of that attempt (using the phony records) and to block any further attempts from that same source(e.g. IP, location etc), this way, when the fraudster will attempt to access the Service Provider's service using real valuable stolen data (and no the fake one sent to it) such usage will be blocked. including *good* details.
6. **Mark & Catch:** For example, the Phishing website to which tries to collect data from the Service Provider's customers, is filled with fake records of people. When the Service Provider detects that these "fake people" attempt to enter the Service Provider's *real* website, the Service Provider can zero in and catch the fraudster
7. issue a press release warning customers against the scam.

When flagging an email as legitimate, the operator can choose between just flagging this specific email as legitimate, or permanently add the suspicious domains or phone numbers in the email as legitimate.

Solution Architecture Example

Various devices and architectures, and sets of devices, may form a system according to various embodiments of the present invention, and my effect a method according to embodiments of the present invention. Methods according to various embodiments of the present invention may, for example, be executed by one or more processors or computing systems (including, for example, memories, processors, software, databases, etc.), which, for example, may be distributed across various sites or computing platforms; alternatively some methods according to embodiments may be executed by single processors or computing systems. The following illustration outlines a solution architecture according to one embodiment of the present invention; other suitable architectures are possible in accordance with other embodiments of the invention:

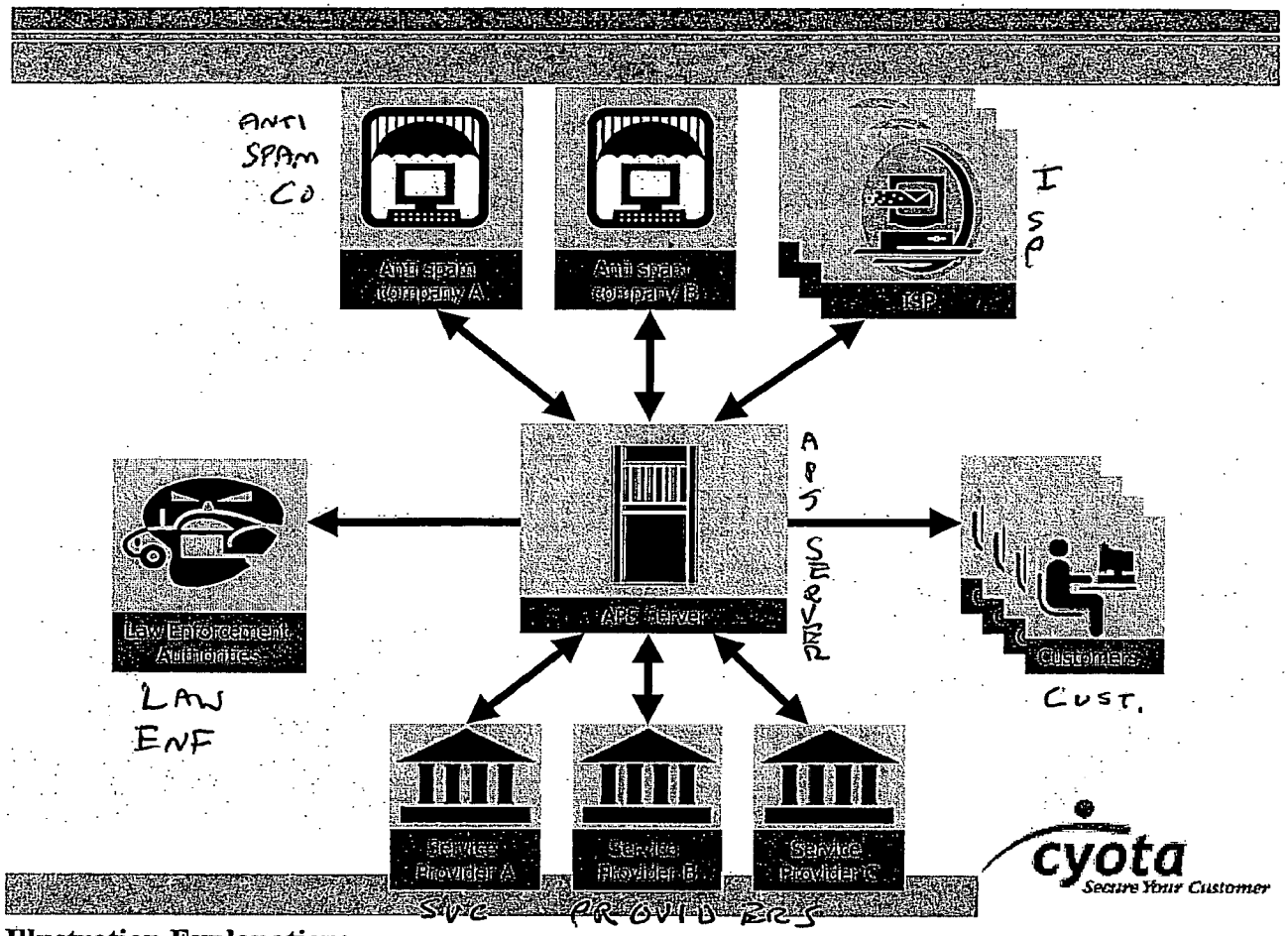

Illustration Explanation:

1. The APS Server - this may be, for example, the central server of the APS service. Operated by, for example, Cyota. This server may for example store the set up, routing information, email server, and the interfaces to the other parties, or other data. While APS Server is used as a term, other suitable servers or systems may be used, and embodiments may be used not involving "Phishing".
2. Service Provider – this may be, for example, the client of the APS service. The Service Provider performs the set up with the APS provider, watches incoming alerts, and instructs how to handle each alert. Other clients may be used.
3. Anti-spam company – this may be, for example, the probe of the APS service – the anti-spam company detects the potential phishing scams and alerts the APS server. It may also help blocking phishing messages.

4. ISP – this may be, for example, an internet service provider – will be contacted by the APS server in case a phishing message should be blocked.
5. Law enforcement authorities – may be contacted by the APS server in case a phishing message is detected to block the site / originating email accounts.
6. Customers or other users - may be contacted by the APS server via email to alert a potential scam.

It will be appreciated by persons skilled in the art that embodiments of the invention are not limited by what has been particularly shown and described hereinabove. Rather the scope of at least one embodiment of the invention is defined by the claims below.

What is claimed is:

1. A system as described herein.
2. A method as described herein.